UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/603,209	06/25/2003	Ulrich Emmerling	071308.0443	2679

31625 7590 01/25/2006

BAKER BOTTS L.L.P.
PATENT DEPARTMENT
98 SAN JACINTO BLVD., SUITE 1500
AUSTIN, TX 78701-4039

EXAMINER	
DWIVEDI, MAHESH H	

ART UNIT	PAPER NUMBER
2168	

DATE MAILED: 01/25/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/603,209	EMMERLING ET AL.	
	Examiner	Art Unit	
	Mahesh H. Dwivedi	2168	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 July 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 July 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/31/2005*. +10/28/03
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement filed 10/28/2003 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because the cited foreign patent document DE 19516992 has no English abstract that was submitted. It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

The information disclosure statement (IDS) submitted on 10/31/2005 has been received, entered into the record, and considered. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

2. The disclosure is objected to because of the following informalities: In page 3, **"between e vehicle an intentionally authorized person with a valid key"** is incoherent. Appropriate correction is required.

Claim Objections

3. Claim 2 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. The claim's subject matter is already explicitly described in claim 1.

Claims 4 and 6 are objected to for incorporating the deficiencies of claim 2.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 3-4, and 12 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The phrase **"if it matches the computation result"** is vague and indefinite as it unclear as to what **"it"** is referring to. Appropriate correction is required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-2, and 11 are rejected under 35 U.S.C. 102(e) as being anticipated by **Stellberger** ("Stellberger" (U.S. Patent 4,509,093)).

Regarding claim 1, **Stellberger** teaches a method comprising:

A) transmitting an item of information unidirectionally between the first object and the at least one further object (Column 6, lines 60-67-Column 7, lines 1-8);

B) calculating a computation result in the relevant receiving object from parts of the transmitted information (Column 7, lines 9-23);

C) comparing the calculated computation result with a computation result transferred with the information (Column 4, lines 22-27, Column 9, lines 32-36); and

D) if there is a match authenticating the vehicle, declaring the computation result as invalid for further transmissions (Column 5, lines 29-31).

The examiner notes that **Stellberger** teaches that the comparison phase can be performed on either the key or the lock. The examiner further notes that it is common knowledge that "random-access memory" (Column 5, lines 29-30) is refreshed after each cycle of inputting data. The examiner further notes that refreshing the data is analogous to declaring the data as **"invalid"**.

Regarding claim 2, **Stellberger** further teaches a method comprising:

A) wherein the information is sent from a vehicle as a first object and received by a key as at least one further object (Column 5, lines 58-61).

Regarding claim 11, **Stellberger** teaches a method comprising:

A) transmitting an item of information unidirectionally between the vehicle and the key (Column 6, lines 60-67-Column 7, lines 1-8);

B) calculating a computation result in the key from parts of the transmitted information (Column 7, lines 9-23);

C) comparing the calculated computation result with a computation result transferred with the information (Column 4, lines 22-27, Column 9, lines 32-36); and

D) if there is a match authenticating the vehicle, declaring the computation result as invalid for further transmissions (Column 5, lines 29-31).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

7. Claims 3-10, and 12-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Stellberger** (U.S. Patent 4,509,093) and in view of **Kocher et al.** (U.S. Patent 6,381,699).

8. Regarding claims 3 and 4, **Stellberger** teaches a method comprising:

A) a random number (Column 5, lines 29-31)

Stellberger, however, does not teach:

B) an incremental or decrementable item of data which is stored in at least one further object if it matches the computation result, is transferred; and

C) after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is sent.

Kocher, however, teaches **"an incremental or decrementable item of data which is stored in at least one further object if it matches the computation result, is transferred"** as "sends other needed information (such as data or t) to the verifier"

(Column 9, lines 23-45), and **"after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is sent"** as "if t matches, the verifier increments t" (Column 9, lines 23-45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher's** would have allowed **Stellberger's** provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Regarding claims 5-6, and 13, **Stellberger** does not explicitly teach a method comprising:

A) wherein a counter state or item of time data is transferred as the item of data that can be incremented.

Kocher, however, teaches **"a counter state or item of time data is transferred as the item of data that can be incremented"** as "counter t" (Column 9, line 24).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher's** would have allowed **Stellberger's** provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Regarding claims 7 and 14, **Stellberger** does not explicitly teach a method comprising:

A) wherein the result is only calculated when the transferred item of data is greater than the stored item of data.

Kocher, however, teaches **"wherein the result is only calculated when the transferred item of data is greater than the stored item of data"** as "if the received value of t is larger than the internal value but the difference is not unreasonably large, it may be appropriate to accept the signature" (Column 9, lines 38-45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher's** would have allowed **Stellberger's** provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Regarding claims 8-9, and 15-16, **Stellberger** does not explicitly teach a method comprising:

A) wherein when the transferred result and the calculated result match, the incrementable item of data is increased so that the transferred result becomes invalid (Column 9, lines 23-45).

Kocher, however, teaches **"wherein when the transferred result and the calculated result match, the incrementable item of data is increased so that the transferred result becomes invalid"** as "if t matches" (Column 9, lines 38-45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher's** would have allowed **Stellberger's** provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Regarding claims 10 and 17, **Stellberger** does not explicitly teach a method comprising:

A) wherein the result is computed in at least one further object using a cryptological computation algorithm known there and a code word (Column 9, lines 8-22).

Kocher, however, teaches **"a code word"** as "symmetrically singed-code" (Column 9, line 10), and "**wherein the result is computed in at least one further object using a cryptological computation algorithm known there"** as "a hash or Mac of the data is typically computed using a secret key" (Column 9, lines 11-22).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher's** would have allowed **Stellberger's** provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Regarding claim 12, **Stellberger** teaches a method comprising:

A) a random number (Column 5, lines 29-31)

B) key (Column 5, lines 58-61)

Stellberger, however, does not teach:

B) an incremental or decrementable item of data which is stored in at least one further object if it matches the computation result, is transferred; and

C) after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is sent.

Kocher, however, teaches **"an incremental or decrementable item of data which is stored in the key if it matches the computation result, is transferred"** as "sends other needed information (such as data or t) to the verifier" (Column 9, lines 23-45), and **"after each transmission of the information, regardless of a successful receipt, the item of data is incremented or decremented before new information is sent"** as "if t matches, the verifier increments t" (Column 9, lines 23-45).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Kocher's** would have allowed **Stellberger's** provide a system of security that remains secure even if attackers gather some information about the system, as noted by **Kocher** (Column 2, lines 40-44).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. PGPUB 20010052075 issued to **Feinberg** on 13 December 2001. The subject matter disclosed therein is pertinent to that of claims 1-17 (e.g., methods to provide device authentication).

U.S. Patent 5,767,784 issued to **Khamhorn** on 16 June 1998. The subject matter disclosed therein is pertinent to that of claims 1-17 (e.g., methods to provide authentication for vehicle entry).

U.S. Patent 5,365,225 issued to **Bachhuber** on 15 November 1994. The subject matter disclosed therein is pertinent to that of claims 1-17 (e.g., methods to provide unidirectional authentication).

U.S. Patent 5,596,641 issued to **Ohashi et al.** on 21 January 1997. The subject matter disclosed therein is pertinent to that of claims 1-17 (e.g., methods to provide remote authentication).

U.S. Patent 4,935,962 issued to **Austin** on 19 June 1990. The subject matter disclosed therein is pertinent to that of claims 1-17 (e.g., methods to provide unidirectional authentication).

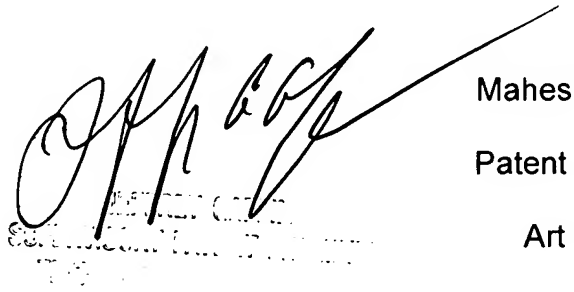
U.S. Patent 4,723,121 issued to **van den Boom et al.** on 02 February 1988. The subject matter disclosed therein is pertinent to that of claims 1-17 (e.g., methods to provide authentication for vehicle entry).

Contact Information

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mahesh Dwivedi whose telephone number is (571) 272-2731. The examiner can normally be reached on Monday to Friday 8:20 am – 4:40 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey Gaffin can be reached (571) 272-4146. The fax number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Mahesh Dwivedi

Patent Examiner

Art Unit 2168

January 17, 2006

Leslie Wong

Primary Examiner